REMARKS

This Amendment is in response to the Office Action dated December 21, 2004. In the Office Action, claim 1-20 were rejected under 35 U.S.C. § 101 as directed towards nonstatutory subject matter. Claims 5, 6, 13, 14, 19 and 20 were rejected under 35 U.S.C. § 112, first paragraph, for failing to comply with the written description requirement. Claims 7 and 8 were rejected under 35 U.S.C. § 112, first paragraph, for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1-3, 9-11, and 15-17 were rejected under 35 U.S.C. § 102(e) as being anticipated by Bugnion et al., U.S. Patent No. 6,496,847 (hereinafter *Bugnion*). Claim 7 was rejected under 35 U.S.C. § 102(a) as being anticipated by Meushaw et al., U.S. Publication No. 2002/0169987 (hereafter *Meushaw*). Claims 4, 5, 12, 13, 18, and 19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Bugnion* as applied to claim 3 above, and further in view of *Meushaw*. Claim 8 was rejected under 35 U.S.C. § 103(a) as being unpatentable over *Meushaw*. Claims 6, 14, and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Bugnion* in view of *Meushaw* as applied to claim 5 above, and further in view of DeTreville, U.S. Patent No. 6,609,199.

Claims 1-3, 7-9, 11, 15, and 17 are amended as shown above. Specifically, independent claims 1, 7, 9, and 15 are amended to more clearly recite features of the claimed invention. Claims 4-6, 10, 12-14, 16, and 18-20 are canceled herein without prejudice. New claims 21-37 have been added. Claims 1-3, 7-9, 11, 15, 17, and 21-37 are now pending in the application. For the reasons set forth below, the Applicants respectfully request reconsideration and allowance of all pending claims.

Objection to Drawings

Substitute drawing sheets comprising formal drawings for each of Figs. 1-4 are attached hereto. No new matter has been added.

Argument in Support of Allowance of the Amended Claims

A claim is anticipated only if each and every element of the claim is found in a single reference. M.P.E.P § 2131 (citing *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628 (Fed. Cir. 1987)). "The identical invention must be shown in as complete detail as is contained in the claim." M.P.E.P. § 2131 (citing *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226 (Fed. Cir. 1989)).

To establish a *prima facie* case of obviousness, there must first be some suggestion or motivation to modify a reference or to combine references, and second be a reasonable expectation of success. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. Third, the prior art reference (or references when combined) must teach or suggest all the claim limitations. M.P.E.P. § 706.02(j) from *In Re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Where claimed subject matter has been rejected as obvious in view of a combination of prior art references, a proper analysis under § 103 requires, *inter alia*, consideration of two factors: (1) whether the prior art would have suggested to those of ordinary skill in the art that they should make the claimed device; and (2) whether the prior art would also have revealed that in so making, those of ordinary skill would have a reasonable expectation of success. Both the suggestion and the reasonable expectation of success must be founded in the prior art, not in the Applicants' disclosure. *Amgen v. Chugai Pharmaceutical*, 927 F.2d 1200, 18 USPQ2d 1016 (Fed. Cir. 1991), *Fritsch v. Lin*, 21 USPQ2d 1731 (Bd. Pat. App. & Int'f 1991). An invention is non-obvious if the references fail not only to expressly disclose the claimed invention as a whole, but also to suggest to one of ordinary skill in the art modifications needed to meet all the claim limitations. *Litton Industrial Products, Inc. v. Solid State Systems Corp.*, 755 F.2d 158, 164, 225 USPQ 34, 38 (Fed. Cir. 1985).

The examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references. M.P.E.P. § 70602(j) from *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985). Obviousness cannot be established by combining references without also providing evidence of the motivating force which would impel one skilled in the art to do what the patent applicant has done. M.P.E.P. § 2144 from *Ex parte Levengood*, 28 USPQ2d 1300, 1302 (Bd. Pat. App. & Inter. 1993) (emphasis added by M.P.E.P.).

Each of independent claims 1, 7, 9, and 15 have been amended to more clearly recite features of the invention to which each claim pertains. Applicant respectfully asserts that each these amended independent claims are patentable over the cited art and are in condition for allowance.

Claim 1, as amended, now recites:

1 A method comprising:

implementing a firmware-based virtual machine monitor (VMM) upon a computing system having a native environment that executes in physical mode; and

emulating legacy hardware components that are not present in the native environment using the VMM to provide support for legacy code that presupposes the existence of such hardware components.

Applicant respectfully assert each and every element of the invention recited in claim 1 is neither taught or suggested by the prior art.

The Background of the Invention section in *Bugnion* gives a detailed overview of how various virtual machine monitors work. In particular, there is a discussion of legacy virtual machine monitors in a section having the same name. Applicable portions of this section (Col. 3, line 58 – Col 4 line 12) are reproduced below:

Legacy Virtual Machine Monitors

...

> A legacy virtual machine monitor consists of the appropriate software support that allows running the legacy operating system using *the special mode of the processor.* ***Specifically, Microsoft's DOS virtual machine runs DOS in a virtual machine on top of Microsoft Windows and NT***. As another example, the freeware DOSEMU system runs DOS ***on top of Linux***.
>
> Although these systems are commonly referred to as a form of virtual machine monitor, ***they run either on top of an existing operating system, such as DOSEMU, or as part of an existing operating system such as Microsoft Windows and Microsoft NT***. In this respect, they are quite different from the true virtual machine monitors described above, and from the definition of the term "virtual machine monitor" applied to the invention described below. (Emphasis added)

Clearly, this conventional legacy VMM is not firmware-based, but rather runs on top of an existing operating system or is part of an existing operating system. This is significant because a software application used to access hardware runs significantly slower than firmware components used to access the same hardware since the software application is layered on an operating system, which, in turn, is layered over a firmware layer sitting between the operating system and the hardware. In addition, implementing a VMM at the software level is not a difficult task, as there are a rich array of memory resources, device drivers and services provided by the operating system. For example, a legacy device may be emulated at the OS level by simply using an OS device driver to perform the emulation.

In contrast, implementing a VMM at the firmware level is significantly more difficult. In particular, this is due to the lack of availability of system resources to the firmware (such as memory page tables and the like), facilities for loading applications into memory, *etc.*

Furthermore, there is no suggestion in any of the references to employ a firmware-based VMM, and simply stating that something that is implemented via software may be likewise implemented via firmware is unsupported and would be rejected by one skilled in the firmware arts. As stated in MPEP 2143.01,

> A statement that modifications of the prior art to meet the claimed invention would have been "'well within the ordinary skill of the art at the time the claimed invention was made'" because the references relied upon teach that all aspects of the claimed invention were individually known in the art is not sufficient to establish a prima facie case of obviousness without some objective reasons to combine the teachings of the references Ex parte Levengood, 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993).

With respect to the patentability of new claim 21, this claim recites,

21. The method of claim 1, further comprising:

loading the VMM during a pre-boot phase of the computer system having an extensible firmware framework, the VMM comprising a modular firmware component running on the extensible firmware framework.

There is no teaching or suggesting in any of the cited references to implement the VMM as a modular firmware component running on an extensible firmware framework. More specifically, *Bugnion* teaches away from such an approach.

A discussion of a conventional VMM architecture that employs a VMM at the system level (*e.g.*, a layer sitting between and operating system and hardware) is disclosed in Col. 6, lines 10-52 of *Bugnion*. Respective parts of this text state,

> As FIG. 1 shows, the VMM 100 communicates directly with the hardware 110 and thus is at system level. (Col. 4, lines 29-30)

and

> Because the VMM 100 in the conventional system shown in FIG. 1 can directly access the hardware 110, it is fast. On the other hand, *because the VMM must be configured according to the given hardware 110, it cannot be used in other systems.* In other words, performance is improved at the cost of less flexibility. (Col. 6, lines 46-52, emphasis added)

The VMM of claim 21 is modular, and is not tied to any underlying hardware. In fact, under the Extensible Firmware Interface (EFI) framework, the VMM does not provide direct access to underlying hardware, but rather is abstracted from the hardware via the EFI core and applicable EFI drivers, wherein the particular set of EFI drivers for a given system are based on the system's hardware configuration. Clearly,

each and every claim element is not taught or suggested by the cited references. Accordingly, claim 21 is patentable over the cited art.

With respect to the patentability of amended independent claim 7, this claim recites,

7. A method comprising:

implementing a virtual machine monitor (VMM) on a computing system having an extensible firmware architecture that enables firmware to be provided from third parties; and

executing untrusted firmware code via the VMM in a sandbox mode during the pre-boot phase of the computer system, wherein the code is given access to a subset of system resources, while code access to other system resources is filtered by the VMM.

In support of the rejection of original claim 7, the Examiner cited *Meushaw*. As recited in the Summary of the Invention section, *Meushaw* states,

> The present invention is a device for and a method of secure computing that includes a computer system on which a host operating-system software program controls resources of the computer system, and a type II virtual machine monitor that ***runs on top of the host operating-system*** to create a user-definable number of virtual machine. (Paragraph 0012, emphasis added)

Clearly, *Meushaw*'s device and method are not implemented using a VMM at the firmware level. Nor does *Meushaw* or any of the other references discuss the use of a VMM during the pre-boot phase of a computer system (that is, the phase prior to the operating system run-time phase at which point an operating system (and all of its resources) are available). Accordingly, amended claim 7 is clearly patentable of the cited art.

With respect to the patentability of amended independent claim 9, this claim is a Beauregard claim that recites a machine-readable medium having executable firmware instructions for performing the method operations of claim 1. Accordingly, amended

claim 9 is patentable over the cited art for reasons similar to those presented above in support of the allowance of claim 1.

With respect to the patentability of amended independent claim 15, this claim is an apparatus claim to a computer system implementing a VMM that performs operations analogous to similar operations recited in amended claim 1. Accordingly, amended claim 9 is patentable over the cited art for reasons similar to those presented above in support of the allowance of claim 1.

With respect to the patentability of new independent claim 27, this claim recites:

27. (New) A method, comprising:

implementing a virtual machine monitor (VMM) during the pre-boot phase of a computer system; and

authenticating an Extensible Firmware Interface (EFI) firmware module using the VMM.

With respect to the *Meushaw* reference, the device and method disclosed therein includes a VMM that is implemented on an operating system. The pre-boot phase corresponds to the phase of a computer system prior to booting an operating system – thus an operating system is not available during the pre-boot phase.

The AEGIS secure bootstrap architecture (A Secure and Reliable Bootstrap Architecture, Arbaugh, Farber, and Smith) is designed to support authentication of conventional expansion card ROMs, and the AEGIS reference was written several years before the first version of the EFI standard became available. The AEGIS secure bootstrap architecture is substantially different from the EFI architecture (*i.e.*, framework), which enables a platform to employ third-party firmware written in accordance with the EFI specification, and is substantially more extensible. Furthermore, the AEGIS reference does not employ or suggest using a VMM . Therefore, it is clear that *Meushaw* and the AEGIS reference, alone or in combination with any of the other cited references, does not teach or suggest each and every

element of new claim 27. Accordingly, claim 27 is patentable and in condition for allowance.

Conclusion

Overall, none of the references singly or in any motivated combination disclose, teach, or suggest what is recited in the independent claims. Thus, given the above amendments and accompanying remarks, independent claims 1, 7, 9, 15, and 27 are now in condition for allowance. The dependent claims that depend directly or indirectly on these independent claims are likewise allowable based on at least the same reasons and based on the recitations contained in each dependent claim.

If the undersigned attorney has overlooked a teaching in any of the cited references that is relevant to the allowability of the claims, the Examiner is requested to specifically point out where such teaching may be found. Further, if there are any informalities or questions that can be addressed via telephone, the Examiner is encouraged to contact the undersigned attorney at (206) 292-8600.

Charge Deposit Account

Please charge our Deposit Account No. 02-2666 for any additional fee(s) that may be due in this matter, and please credit the same deposit account for any overpayment.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Date: March 21, 2005

R. Alan Burnett
Reg. No. 46,149

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1030